OPC UA Configuration Manager

Inhaltsverzeichnis

OPC UA Configuration Manager 1
Inhaltsverzeichnis 2
OPC UA Configuration Manager 4
Übersicht 4
OPC UA Configuration Manager 5
Projekteigenschaften – OPC UA 5
Serverendpunkte 7
Vertrauenswürdige Clients 9
Ermittlungsserver 9
Vertrauenswürdige Server 10
Instanzzertifikate 12
OPC UA Lernprogramm 15
Verbindungsbeispiele 25
Tipps zur Problembehandlung 27
Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen 27
Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird 27
Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden 28
Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort) 28
Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden 28
Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll 28
Ereignisprotokollmeldungen 30
Konto '<Name>' hat keine Berechtigung zum Ausführen der Anwendung. 30
Das Zertifikat des UA Server wurde erneut ausgestellt. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. 30
Das Zertifikat des UA Client Treibers wurde erneut ausgestellt. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. 30
Das UA Client Zertifikat '<Client-Name>' wurde zurückgewiesen. Der Server kann keine Verbindungen von dem Client annehmen. 30
Das UA Client Zertifikat '<Client-Name>' wurde als vertrauenswürdig eingestuft. Der Server kann Verbindungen von dem Client annehmen. 30
Das UA Server Zertifikat '<Servername>' wurde zurückgewiesen. Der UA Client Treiber kann keine Verbindung zum Server herstellen. 31
Das UA Server Zertifikat '<Servername>' wurde als vertrauenswürdig eingestuft. Der UA Client Treiber kann eine Verbindung zum Server herstellen. 31
Das UA Server Zertifikat '<Servername>' wurde zur Liste der vertrauenswürdigen Server hinzugefügt. Der UA Client Treiber kann jetzt eine Verbindung zum Server herstellen. 31
Das UA Client Zertifikat '<Client-Name>' wurde zur Liste der vertrauenswürdigen Clients hinzugefügt. Der UA Server kann jetzt Verbindungen vom Client annehmen. 31
Das UA Client Zertifikat '<Client-Name>' wurde aus der Liste der vertrauenswürdigen Clients entfernt. Der UA Server kann keine Verbindungen vom Client annehmen. 31

Das UA Server Zertifikat '<Servername>' wurde aus der Liste der vertrauenswürdigen Server entfernt. Der UA Client Treiber kann keine Verbindung zum Server herstellen. ... 31
Der Endpunkt '<URL>' wurde zum UA Server hinzugefügt. ... 31
Der Endpunkt '<URL>' wurde vom UA Server entfernt. ... 31
Der UA Discovery Server '<Servername>' wurde hinzugefügt. Die UA Server Endpunkte können jetzt mit diesem UA Discovery Server registriert werden. ... 31
Der UA Discovery Server '<Servername>' wurde entfernt. Die UA Server Endpunkte können nicht länger mit diesem UA Discovery Server registriert werden. ... 32
Der Endpunkt '<URL>' wurde deaktiviert. ... 32
Das Zertifikat des UA Client Treibers wurde importiert. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. ... 32
Das Zertifikat des UA Server wurde importiert. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. ... 32
Der Endpunkt '<URL>' wurde aktiviert. ... 32
Vertrauenswürdigen Client hinzufügen ... 32
Vertrauenswürdigen Client entfernen ... 32
Vertrauenswürdigen Client ablehnen ... 32
Vertrauenswürdigem Client vertrauen ... 32
Vertrauenswürdigen Server hinzufügen ... 32
Vertrauenswürdigen Server entfernen ... 32
Vertrauenswürdigen Server ablehnen ... 33
Vertrauenswürdigem Server vertrauen ... 33
Endpunkt hinzufügen ... 33
Endpunkt aktivieren ... 33
Endpunkt deaktivieren ... 33
Endpunkt entfernen ... 33
Ermittlungsserver hinzufügen ... 33
Ermittlungsserver entfernen ... 33
Client-Zertifikat erneut ausstellen ... 33
Serverzertifikat erneut ausstellen ... 33
Index ... **34**

OPC UA Configuration Manager

Hilfe-Version 1.042

INHALT

Übersicht
Was ist OPC Unified Architecture und wie wird sie verwendet?

OPC UA Configuration Manager
Wo finde ich Informationen zu den Registerkarten in OPC UA Configuration Manager ?

OPC UA Lernprogramm
Wo finde ich ein Lernprogramm zur Implementierung von OPC UA?

Verbindungsbeispiele
Wo finde ich Beispiele für Verbindungen und Informationen zu optimalen Vorgehensweisen im Zusammenhang mit OPC UA?

Tipps zur Problembehandlung
Wo finde ich Beschreibungen zu häufigen Problemen?

Ereignisprotokollmeldungen
Welche Meldungen enthält das Ereignisprotokoll?

Übersicht

OPC Unified Architecture (UA) ist ein offener Standard, der durch die OPC Foundation mit Unterstützung Dutzender von Mitgliedsorganisationen erstellt wurde. Obgleich UA beabsichtigt, einen plattformunabhängigen Interoperabilitätsstandard bereitzustellen (weg von Microsoft COM) stellt UA keinen Ersatz für OPC Data Access (DA) Technologien dar. Für die meisten Industrieanwendungen ergänzt oder erweitert UA eine bestehende DA-Architektur. Es handelt sich nicht um einen systemweiten Ersatz. OPC UA ergänzt OPC DA Infrastrukturen auf folgende Weise:

- UA bietet auch eine sichere Methode für die Konnektivität zwischen Client und Server, ohne von Microsoft DCOM abhängig zu sein, und ermöglicht, durch Firewalls und über VPN-Verbindungen eine sichere Verbindung herzustellen. Für Benutzer, die innerhalb eines Unternehmensnetzwerks (innerhalb der Firewall) auf einer Domäne eine Verbindung zu einem Remote-Computer herstellen, sind OPC DA und eine DCOM-Verbindung möglicherweise ausreichend.
- Sie stellt eine zusätzliche Möglichkeit bereit, Fabrikdaten gemeinsam für Geschäftssysteme zu nutzen (von der Fabrik bis zur obersten Ebene). OPC UA kann Daten aus mehreren OPC DA-Quellen in Nicht-Industriesystemen aggregieren.

Für die Mehrzahl von Benutzeranwendungen sind dies die relevantesten Komponenten des UA-Standards:

- Sichere Verbindungen über vertrauenswürdige Zertifikate für Client- und Serverendpunkte
- Robustes Element-Abonnement-Modell, für das Bereitstellen effizienter Datenaktualisierungen zwischen Clients und Servern
- Eine verbesserte Methode zum Ermitteln verfügbarer Informationen von beteiligten UA-Servern

OPC UA Configuration Manager

Der OPC UA Configuration Manager hilft Benutzern bei der Verwaltung der Konfigurationseinstellungen für den UA Server. Die Sicherheit für OPC UA erfordert, dass alle an der UA-Kommunikation beteiligten Endpunkte über eine sichere Verbindung kommunizieren. Um diese Sicherheitsanforderung zu erfüllen, muss jede UA Server-Instanz und jede UA Client-Instanz ein vertrauenswürdiges Zertifikat bereitstellen, um sich zu identifizieren. Diese Zertifikate können selbstsigniert sein. Als solche müssen sie dem lokalen vertrauenswürdigen Zertifikatspeicher sowohl auf den Server- als auch auf den Client-Knoten durch einen Benutzer mit Administratorberechtigungen hinzugefügt werden, bevor versucht werden kann, sichere UA Client-/Server-Verbindungen herzustellen. Der OPC UA Configuration Manager ist eine benutzerfreundliche Benutzeroberfläche, über die der Zertifikataustausch durchgeführt werden kann.

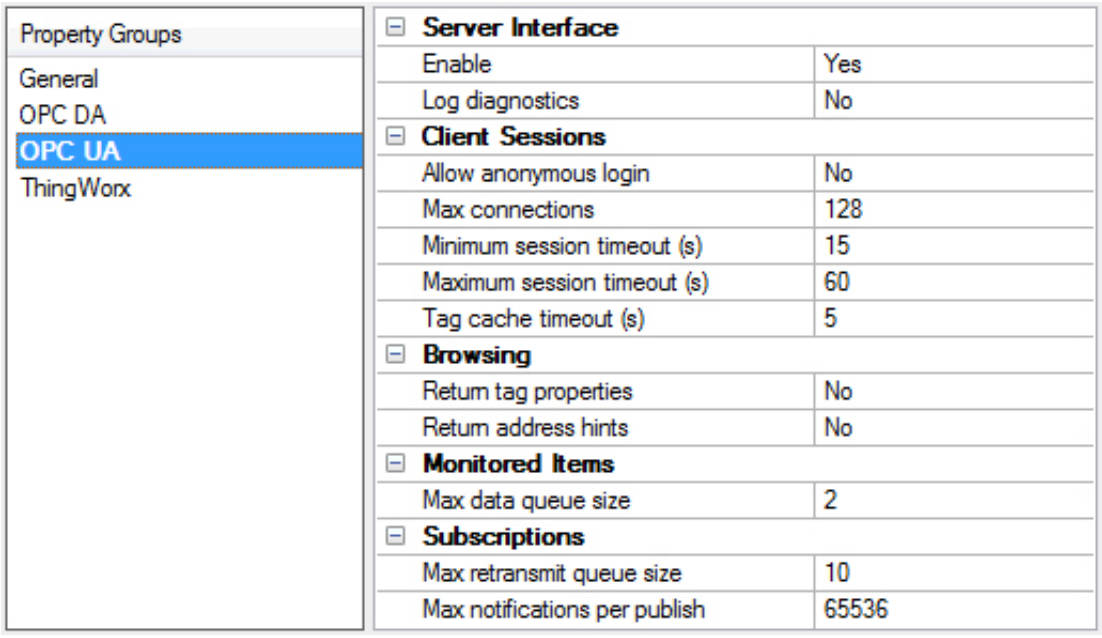
Weitere Informationen zu einer spezifischen OPC UA Configuration Manager Eigenschaft finden Sie unter den nachfolgenden Links.

Serverendpunkte
Vertrauenswürdige Clients
Ermittlungsserver
Vertrauenswürdige Server
Instanzzertifikate

Projekteigenschaften - OPC UA

OPC Unified Architecture (UA) stellt einen plattformunabhängigen Interoperabilitätsstandard bereit. Sie stellt keinen Ersatz für OPC Data Access (DA)-Technologien dar: für die meisten Industrieanwendungen ergänzt oder erweitert UA eine bestehende DA-Architektur. Die OPC UA-Projekteigenschaften-Gruppe zeigt die aktuellen OPC UA-Einstellungen im Server an.

Hinweis: Um eine Einstellung zu ändern, klicken Sie in die zweite Spalte der jeweiligen Eigenschaft. Dadurch wird ein Dropdown-Menü aufgerufen, das die zur Verfügung stehenden Optionen anzeigt.



Serverschnittstelle

Aktivieren: Bei Aktivierung wird die UA-Serverschnittstelle initialisiert und akzeptiert Client-Verbindungen. Sofern deaktiviert, sind die übrigen Eigenschaften auf dieser Seite deaktiviert.

Protokolldiagnose: Bei Aktivierung werden OPC UA-Stapeldiagnosen im OPC Diagnostics Viewer protokolliert. Diese Option sollte nur zu Fehlerbehebungszwecken aktiviert werden.

Client-Sitzungen

Anonyme Anmeldung zulassen: Diese Eigenschaft gibt an, ob zum Herstellen einer Verbindung Benutzername und Passwort erforderlich sind. Aus Gründen der Sicherheit lautet die Standardeinstellung "Nein", um keinen anonymen Zugriff zu erlauben und Anmeldeinformationen zu verlangen.
Hinweis: Wenn diese Einstellung deaktiviert ist, können sich Benutzer nicht als Standardbenutzer im Benutzermanageranmelden. Benutzer können sich als Administrator unter der Voraussetzung anmelden, dass ein Passwort im Benutzermanager festgelegt und zur Anmeldung verwendet wird.
Tipp: Zusätzliche Benutzer können so konfiguriert werden, dass sie auf Daten ohne sämtliche Berechtigungen zugreifen können, die dem Administratorkonto zugeordnet sind. Stellt der Client beim Verbindungsaufbau ein Passwort bereit, so verschlüsselt der Server das Passwort und verwendet hierzu einen Verschlüsselungsalgorithmus, der von der Sicherheitsrichtlinie des Endpunkts definiert ist, und meldet sich anschließend damit an.
Note: Users can login as the Administrator using the password set during the installation of KEPServerEXOPC AggregatorThingWorx Kepware ServerThingWorx Kepware Edge to login. Additional users may be configured to access data without all the permissions associated with the administrator account. When the client supplies a password on connect, the server decrypts the password using the encryption algorithm defined by the security policy of the endpoint, then uses it to login.
Stellt der Client beim Verbindungsaufbau ein Passwort bereit, so verschlüsselt der Server das Passwort und verwendet hierzu einen Verschlüsselungsalgorithmus, der von der Sicherheitsrichtlinie des Endpunkts definiert ist.

Max. Verbindungen: Legen Sie die maximale Anzahl unterstützter Verbindungen fest. Der gültige Bereich liegt zwischen 1 und 128. Die Standardeinstellung ist 128.

Mindestwert für Sitzungs-Timeout: Legen Sie den Mindestwert für das Timeout des UA-Clients beim Einrichten einer Sitzung fest. Werte können ggf. abhängig von den Anforderungen der Anwendung geändert werden. Der Standardwert ist 15 Sekunden.

Höchstwert für Sitzungs-Timeout: Legen Sie den Höchstwert für das Timeout des UA-Clients beim Einrichten einer Sitzung fest. Werte können ggf. abhängig von den Anforderungen der Anwendung geändert werden. Der Standardwert ist 60 Sekunden.

Tag-Cache-Timeout: Legen Sie das Tag-Cache-Timeout fest. Der gültige Bereich liegt zwischen 0 und 60 Sekunden. Die Standardeinstellung ist 5 Sekunden.
Hinweis: Dieser Timeout steuert, wie lange ein Tag zwischengespeichert wird, nachdem ein UA-Client damit fertig ist, es zu verwenden. In Fällen, wo UA-Clients in einem festgelegten Intervall in nicht registrierte(n) Tags lesen/schreiben, können Benutzer die Leistung durch Erhöhen des Timeouts verbessern. Beispiel: Wenn ein Client ein nicht registriertes Tag alle 5 Sekunden liest, sollte der Tag-Cache-Timeout auf 6 Sekunden festgelegt werden. Da das Tag während jeder Client-Anforderung nicht neu erstellt werden muss, verbessert sich die Leistung.

Durchsuchen

Return Tag Properties: Aktivieren Sie diese Option, um UA-Client-Anwendungen die für jedes Tag im Adressraum verfügbaren Tag-Eigenschaften durchsuchen zu lassen. Diese Einstellung ist standardmäßig deaktiviert.

Adresshinweise zurückgeben: Aktivieren Sie diese Option, um UA-Client-Anwendungen die für jedes Element verfügbaren Adressformatierungshinweise durchsuchen zu lassen. Zwar handelt es sich bei den Hinweisen um keine gültigen UA-Tags, doch bestimmte UA-Client-Anwendungen versuchen möglicherweise, sie zur Tag-Datenbank hinzuzufügen. Wenn dies vorkommt, erhält der Client einen Fehler vom Server. Dies hat möglicherweise zur Folge, dass der Client Fehler berichtet oder keine Tags mehr automatisch hinzufügt. Um zu verhindern, dass dies auftritt, stellen Sie sicher, dass diese Eigenschaft deaktiviert ist. Diese Einstellung ist standardmäßig deaktiviert.

Überwachte Elemente

Max. Data Queue Size: Legen Sie die maximale Anzahl der Datenbenachrichtigungen fest, die für ein Element in die Warteschlange gestellt werden. Der gültige Bereich liegt zwischen 1 und 100. Die Standardeinstellung ist 2.
Hinweis: Die Datenwarteschlange wird verwendet, wenn das Aktualisierungsintervall des überwachten

Elements schneller als das Publizierungsintervall des Abonnements ist. Beispiel: Wenn das Aktualisierungsintervall des überwachten Elements 1 Sekunde ist und ein Abonnement alle 10 Sekunden publiziert wird, werden 10 Datenbenachrichtigungen für das Element alle 10 Sekunden publiziert. Da Speicher verbraucht wird, wenn Daten in die Warteschlange gestellt werden, sollte dieser Wert begrenzt werden, wenn der Speicher ein Problem darstellt.

Abonnements

Max. Retransmit Queue Size: Legen Sie die maximale Anzahl von Publizierungen fest, die pro Abonnement in die Warteschlange gestellt werden. Der gültige Bereich liegt zwischen 1 und 100. Der Wert Null deaktiviert erneute Übertragungen. Die Standardeinstellung ist 10.
Hinweis: Ereignisse zum Publizieren des Abonnements werden auf Anforderung des Clients in die Warteschlange gestellt und erneut übertragen. Da Speicher verbraucht wird, wenn die Warteschlange verwendet wird, sollte dieser Wert begrenzt werden, wenn der Speicher ein Problem darstellt.

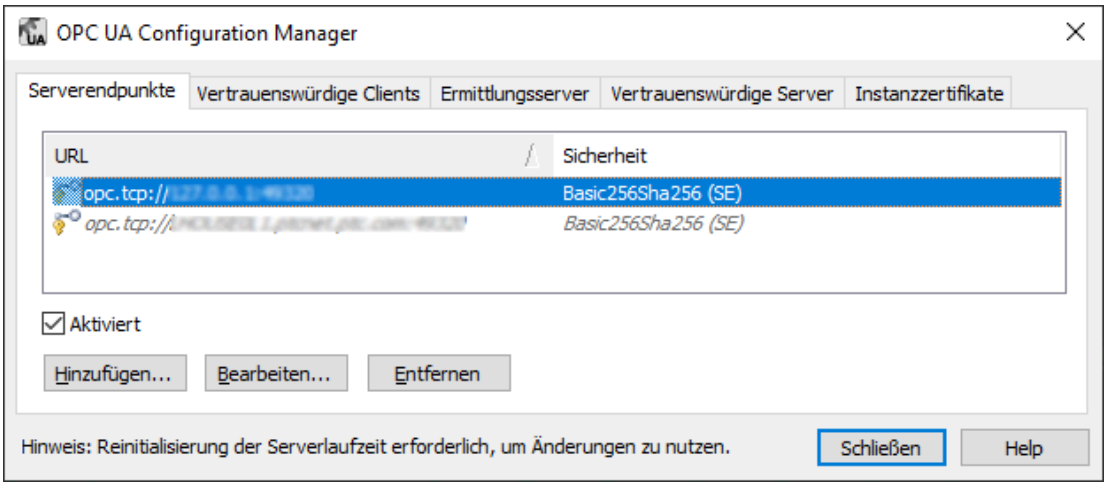
Max. Notifications Per Publish: Legen Sie die maximale Anzahl von Benachrichtigungen pro Publizierung fest. Der gültige Bereich liegt zwischen 1 und 65536. Die Standardeinstellung ist 65536.
Hinweis: Dieser Wert wirkt sich möglicherweise auf die Leistung der Verbindung aus, indem die Größe der vom Server an den Client gesendeten Pakete begrenzt wird. Im Allgemeinen sollten große Werte für Verbindungen mit hoher Bandbreite und kleine Werte für Verbindungen mit niedriger Bandbreite verwendet werden.

Die Schaltfläche **Standardeinstellungen** setzt die Einstellungen auf die Standardwerte/voreingestellten Werte zurück.

Serverendpunkte

Der OPC UA Server erfordert Serverendpunkt-Definitionen, um eine UA Benutzeroberfläche zu erstellen, mit der UA-Clients kommunizieren können. UA-Server-Endpunkte sind als URLs (Universal Resource Locators) definiert und identifizieren die bestimmte Instanz eines Servers, Transporttyps, sowie die Sicherheit, mit der kommuniziert wird. Ein Serverendpunkt besteht aus einer URL und einem Sicherheitsrichtlinien-Typ. Es sind maximal 100 Serverendpunkte in einem Projekt erlaubt. Die Registerkarte "Serverendpunkte" zeigt u.U. mehrere Serverendpunkte in einer Zeile an.

Hinweis: Jeder neu definierte Endpunkt ist standardmäßig aktiviert, kann jedoch, falls gewünscht, vom Benutzer deaktiviert werden. Werden Endpunkte hinzugefügt, entfernt oder geändert, während der Server ausgeführt wird, so muss die Laufzeit des UA Servers neu initialisiert werden.



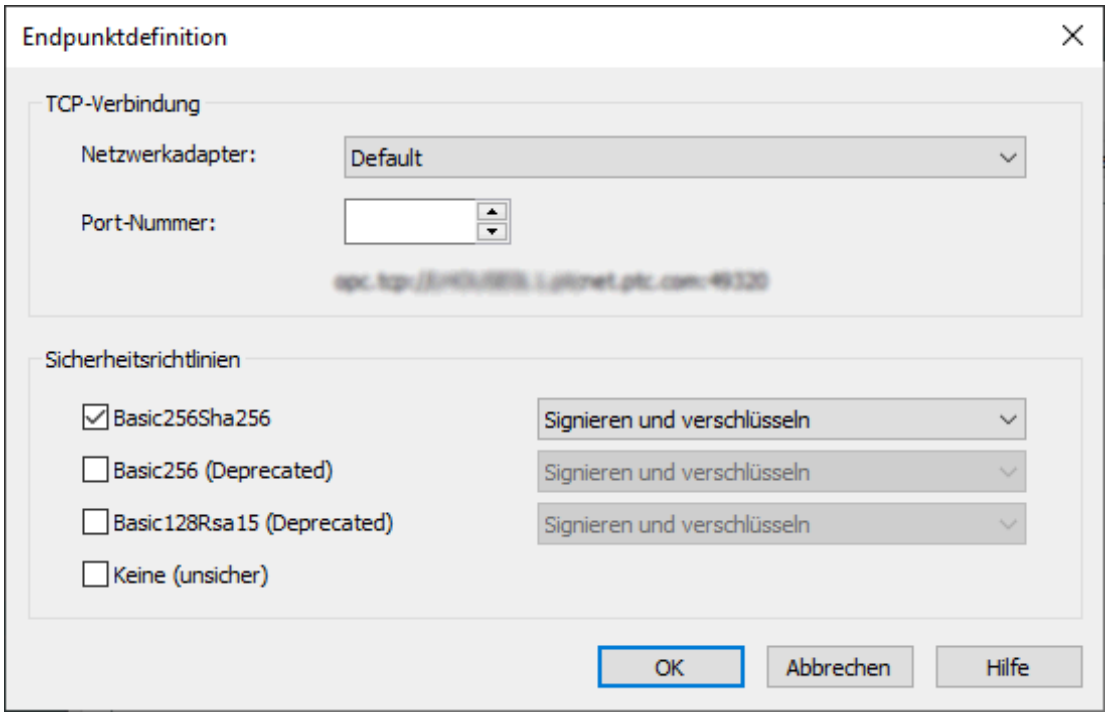
Hinweis: Alle Endpunkte innerhalb der Serverinstanz teilen dasselbe Instanzzertifikat. Der UA Server verwendet standardmäßig selbstsignierte Zertifikate, Benutzer können jedoch auf der Registerkarte Instanzzertifikate eine benutzerdefinierte Instanz importieren.

Wichtig: Gemäß den OPC UA Anforderungen, muss ein Server, welcher das standardmäßige UA Server-Profil implementiert, das Anmelden mit Benutzername und Passwort unterstützen. Dieser UA Server unterstützt die Validierung von Benutzerinformationen pro Serverinstanz (anstatt von pro Endpunkt). Erkannte Benutzer

stammen aus der Funktion "Benutzermanager" innerhalb der Serververwaltung, die sich in der Taskleiste befindet.

Endpunktdefinition

Klicken Sie auf der Registerkarte "Serverendpunkte" auf **Hinzufügen...** oder **Bearbeiten...** um das Dialogfenster "Endpunktdefinition" zu öffnen.



Netzwerkadapter: Dieser Parameter gibt den Netzwerkadapter, an den die Verbindung gebunden wird, an. Er kann für verfügbare Adapter mit IP-Adressen, Standard oder lediglich lokalen Host konfiguriert werden. Die anfängliche Auswahl ist Standard, d.h. es wird eine Zuordnung zu einem Standard-Netzwerkadapter hergestellt.

Port-Nummer: Dieser Parameter gibt die Port-Nummer an. Dieser Parameter ist für die Definition erforderlich, da der restliche Teil der URL, welche für die Definition des Endpunkts konstruiert ist, auf dem Hostnamen des Computers und dem Transportprotokoll standardisiert ist. Alle von diesem Dialogfenster definierten Endpunkt-URLs haben das folgende Format: *opc.tcp://<Hostname>:<Port>*. Für den Fall, dass kein vollständig qualifizierter Hostname bestimmt werden kann, wird entweder der lokale Host oder eine IP-Adresse verwendet.

Sicherheitsrichtlinien: Diese Sicherheitsrichtlinien- und Meldungsmodus-Parameter geben die vom UA Server unterstützten Sicherheitsalgorithmen an. Basic256Sha256 ist standardmäßig ausgewählt. Die folgenden Optionen sind möglich:

- Basic256Sha256
- Basic256 (Deprecated)
- Basic128Rsa15 (Deprecated)
- Keine (unsicher)

Auf das Dropdown-Menü für die Sicherheitsrichtlinie kann nur dann zugegriffen werden, wenn das entsprechende Kontrollkästchen aktiviert ist. Ist keine der Sicherheitsrichtlinien aktiviert, so wird angenommen, dass die Standard-Sicherheitsrichtlinie "Keine" ist. Diese Auswahl wird nicht empfohlen, da sie keine Sicherheit bietet. Jedes Dropdown-Menü listet die Verschlüsselungsmodi, die vom UA Server unterstützt werden, auf. Sortiert sind die Modi in absteigender Reihenfolge, d.h. von am sichersten bis am wenigsten sicher. Die Standardauswahl ist "Signieren und verschlüsseln". Die folgenden Optionen sind möglich:

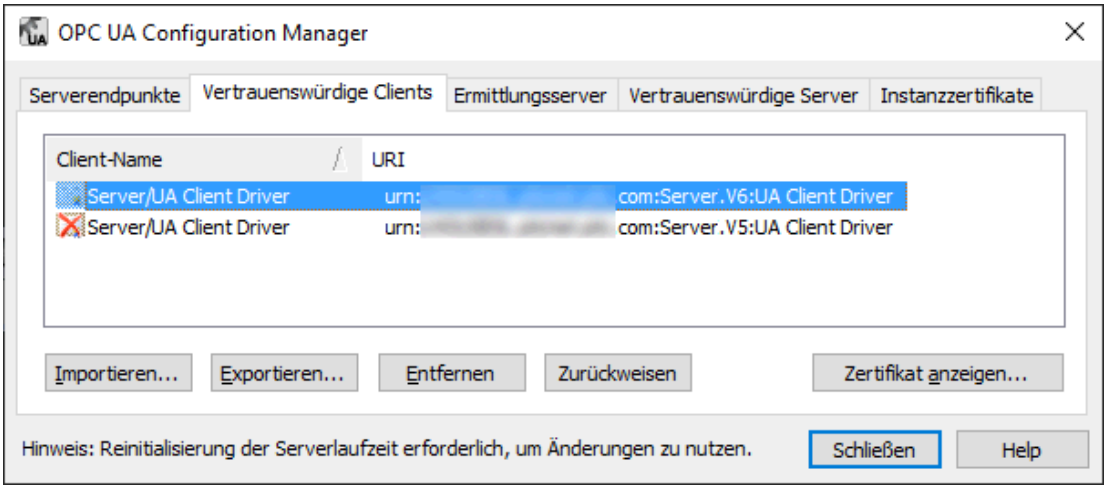
- Signieren und verschlüsseln
- Signieren; Signieren und verschlüsseln

- Signieren

ACHTUNG: Die Sicherheitsrichtlinien Basic128Rsa15 und Basic256 werden von der OPC Foundation ab der OPC UA-Spezifikation Version 1.04 als veraltet angesehen. Die von diesen Richtlinien bereitgestellte Verschlüsselung ist weniger sicher und die Verwendung der Richtlinien sollte auf das Bereitstellen von Abwärtskompatibilität beschränkt werden.

Vertrauenswürdige Clients

UA Server benötigen ein Zertifikat, um eine vertrauenswürdige Verbindung zu jedem UA-Client herzustellen. Damit der Server Verbindungen von einem Client mit selbstsigniertem Zertifikat akzeptiert, muss das Zertifikat des Clients in den Zertifikatspeicher des vertrauenswürdigen Client, der von der OPC UA Server Benutzeroberfläche verwendet wird, importiert werden. Um dies zu ermöglichen, kann der UA Configuration Manager vertrauenswürdige Client-Zertifikate importieren, entfernen und anzeigen.



Importieren...: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Client-Zertifikat importiert.

Exportieren...: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Client-Zertifikat an einen gewünschten Speicherort exportiert.

Entfernen: Wird diese Schaltfläche geklickt, so wird das Vertrauen aus dem Client-Zertifikat entfernt. Außerdem wird das Zertifikat aus der Liste der vertrauenswürdigen Clients entfernt.

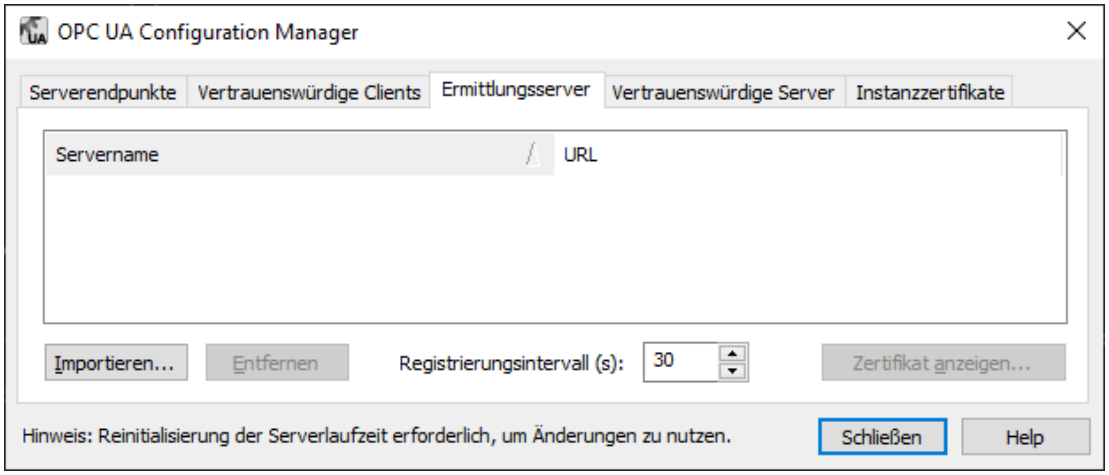
Zurückweisen: Wird diese dynamische Schaltfläche geklickt, so wird Vertrauen aus einem Client-Zertifikat entfernt. Zurückgewiesene Zertifikate verbleiben in der Liste der vertrauenswürdigen Clients und werden mit einem roten X gekennzeichnet.

Vertrauen: Wird diese dynamische Schaltfläche geklickt, so wird einem Client-Zertifikat vertraut.

Zertifikat anzeigen...: Wird diese Schaltfläche geklickt, so werden Informationen zum Client-Zertifikat angezeigt.

Ermittlungsserver

Jeder OPC UA-Server kann sich mit einem UA-Ermittlungsserver registrieren, damit Clients mit den entsprechenden Berechtigungen auf seine Endpunkt-Informationen zugreifen können. Für das Durchführen dieser Registrierung muss die UA-Server-Benutzeroberfläche wissen, welcher Endpunkt bzw. welche Endpunkte verwendet werden sollen. Ein Ermittlungsserver mit einem selbstsignierten Zertifikat muss abgerufen und im vertrauenswürdigen Zertifikatspeicher des UA-Servers gespeichert werden. Desgleichen muss das Zertifikat des UA-Servers abgerufen werden und im vertrauenswürdigen Zertifikatspeicher des UA-Ermittlungsservers gespeichert werden. OPC UA Configuration Manager ermöglicht das Importieren, Entfernen und Anzeigen vertrauenswürdiger Ermittlungsserver-Endpunkte, die für die UA-Server-Benutzeroberfläche identifiziert werden.

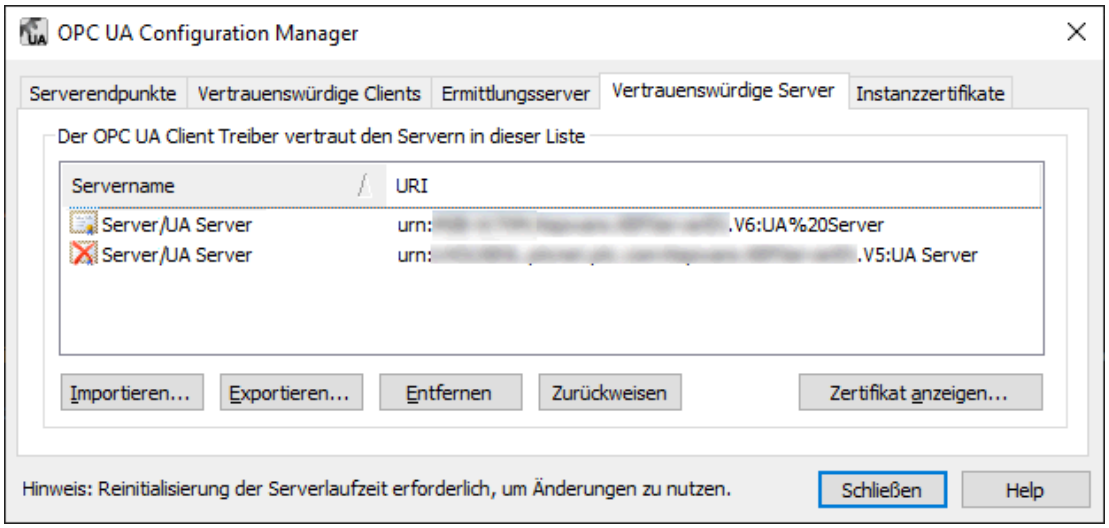


Hinweis: Benutzer können das Registrierungsintervall, welches zum Aktualisieren des Ermittlungsservers verwendet wird, über den Parameter **Registrierungsintervall** ändern. Die Standardeinstellung ist 30 Sekunden.

Vertrauenswürdige Server

Die Registerkarte "Vertrauenswürdige Server" wird nur angezeigt, wenn der UA Client-Treiber auf dem Computer installiert ist. Das Dialogfenster wird verwendet, um eine Liste von vertrauenswürdigen Servern, mit denen der UA Client-Treiber kommunizieren kann, zu erstellen.

Hinweis: Der UA Client-Treiber erfordert eine vertrauenswürdige Zertifikatsverwaltung für Clients, die selbst signieren, genau wie der UA Server. Damit der UA Client-Treiber eine Verbindung zu einem Server, der ein selbstsigniertes Zertifikat verwendet, herstellen kann, müssen Benutzer mit Administratorberechtigungen das Zertifikat des externen UA Servers in den vertrauenswürdigen Zertifikatspeicher des UA Client-Treibers importieren. Da der Client-Treiber sein Zertifikat selbst signiert, muss dieses Zertifikat exportiert und im vertrauenswürdigen Zertifikatspeicher des Servers gespeichert werden.



Importieren...: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Serverzertifikat importiert.

Exportieren...: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Serverzertifikat an einen gewünschten Speicherort exportiert.

Entfernen: Wird diese Schaltfläche geklickt, so wird das Vertrauen aus dem Serverzertifikat entfernt. Außerdem wird das Zertifikat aus der Liste der vertrauenswürdigen Server entfernt.

Zurückweisen: Wird diese dynamische Schaltfläche geklickt, so wird Vertrauen aus einem Serverzertifikat entfernt. Zurückgewiesene Zertifikate verbleiben in der Liste der vertrauenswürdigen Server und werden mit einem roten X gekennzeichnet.

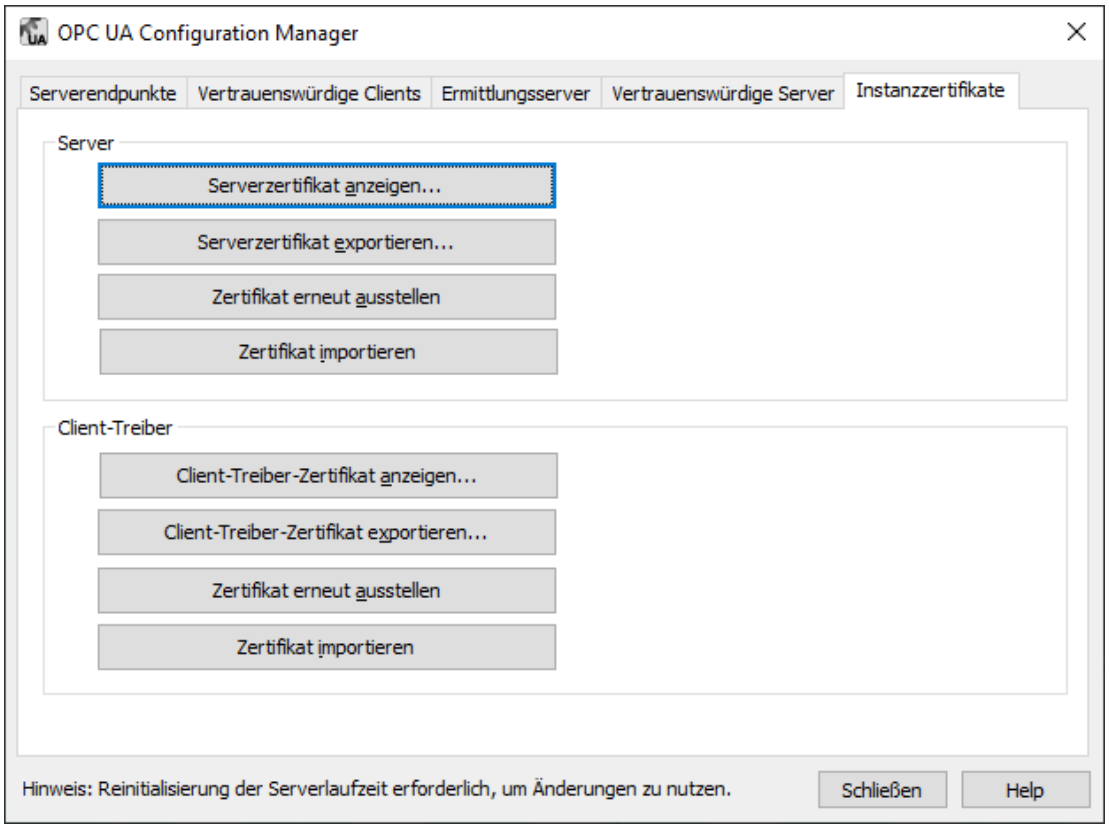
Vertrauen: Wird diese dynamische Schaltfläche geklickt, so wird einem Serverzertifikat vertraut.

Zertifikat anzeigen…: Wird diese Schaltfläche geklickt, so werden Informationen zum Serverzertifikat angezeigt.

Anweisungen zum Austausch von Zertifikaten zwischen UA Client-Treiber und UA Server finden Sie unter ***Manueller Austausch****.*

Instanzzertifikate

Die selbstsignierten X.509-Instanzzertifikate wurden für den UA Server und die UA Client-Treiber geschaffen. Auf sie kann über die Registerkarte "Instanzzertifikate", wie nachfolgend gezeigt, zugegriffen werden.



Server

Serverzertifikat anzeigen: Wird diese Schaltfläche geklickt, so wird das Serverzertifikat aufgerufen. Das Dialogfenster enthält neben dem Zertifikationspfad sowohl allgemeine wie auch detaillierte Zertifikatinformationen. *Weitere Informationen dazu finden Sie unter*Zertifikatanzeige.

Serverzertifikat exportieren: Wird diese Schaltfläche geklickt, so wird das Serverzertifikat an den gewünschten Speicherort exportiert.

Zertifikat erneut ausstellen: Wird diese Schaltfläche geklickt, so wird das Serverzertifikat erneut ausgestellt. Von OPC UA Configuration Manager generierte Zertifikate sind selbstsigniert, für die Signatur wurde der rsa-sha256-Algorithmus verwendet, und sie laufen nach 3 Jahren aus. Durch eine erneute Ausstellung werden vorhandene Vertrauensbeziehungen ungültig.

Zertifikat importieren: Wird diese Schaltfläche geklickt, so wird ein Zertifikat importiert. Importierte Serverzertifikate müssen das Format PKCS12 (eine .pfx-Erweiterung) aufweisen. Sie müssen sowohl das Instanzzertifikat als auch den privaten Schlüssel enthalten und können passwortgeschützt sein.

Client

Client-Treiber-Zertifikat anzeigen: Wird diese Schaltfläche geklickt, so wird das Client-Treiber-Zertifikat aufgerufen. Das Dialogfenster enthält neben dem Zertifikationspfad sowohl allgemeine wie auch detaillierte Zertifikatinformationen. *Weitere Informationen dazu finden Sie unter*Zertifikatanzeige.

Client-Treiber-Zertifikat exportieren: Wird diese Schaltfläche geklickt, so wird das Client-Treiber-Zertifikat an den gewünschten Speicherort exportiert.

Zertifikat erneut ausstellen: Wird diese Schaltfläche geklickt, so wird das Client-Treiber-Zertifikat erneut ausgestellt. Von OPC UA Configuration Manager generierte Zertifikate sind selbstsigniert, für die Signatur wurde

der rsa-sha256-Algorithmus verwendet, und sie laufen nach 3 Jahren aus. Durch eine erneute Ausstellung werden vorhandene Vertrauensbeziehungen ungültig.

Zertifikat importieren: Wird diese Schaltfläche geklickt, so wird ein Zertifikat importiert. Importierte Client-Zertifikate müssen das Format PKCS12 (eine .pfx-Erweiterung) aufweisen. Sie müssen sowohl das Instanzzertifikat als auch den privaten Schlüssel enthalten und können passwortgeschützt sein.

Selbstsignierte Standard-Zertifikate

Dateinamen:

- <Produktname>_ua_server.der
- <Produktname>_ua_client_driver.der

Ablaufdatum:

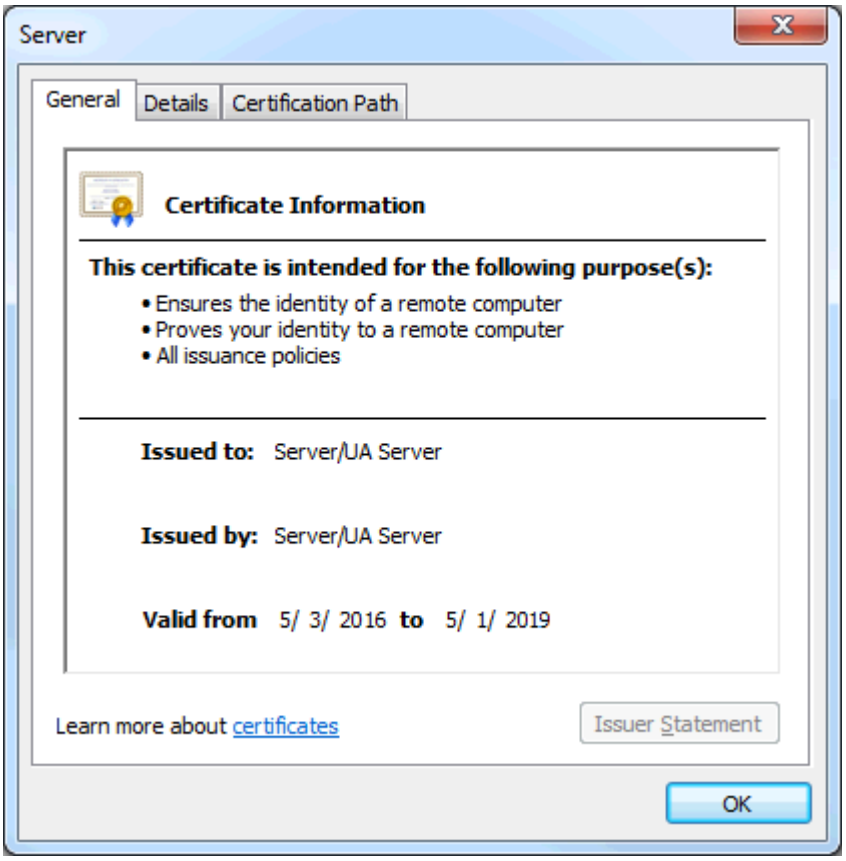
- Drei (3) Jahre nach Ausstellung.

Signier-Algorithmus

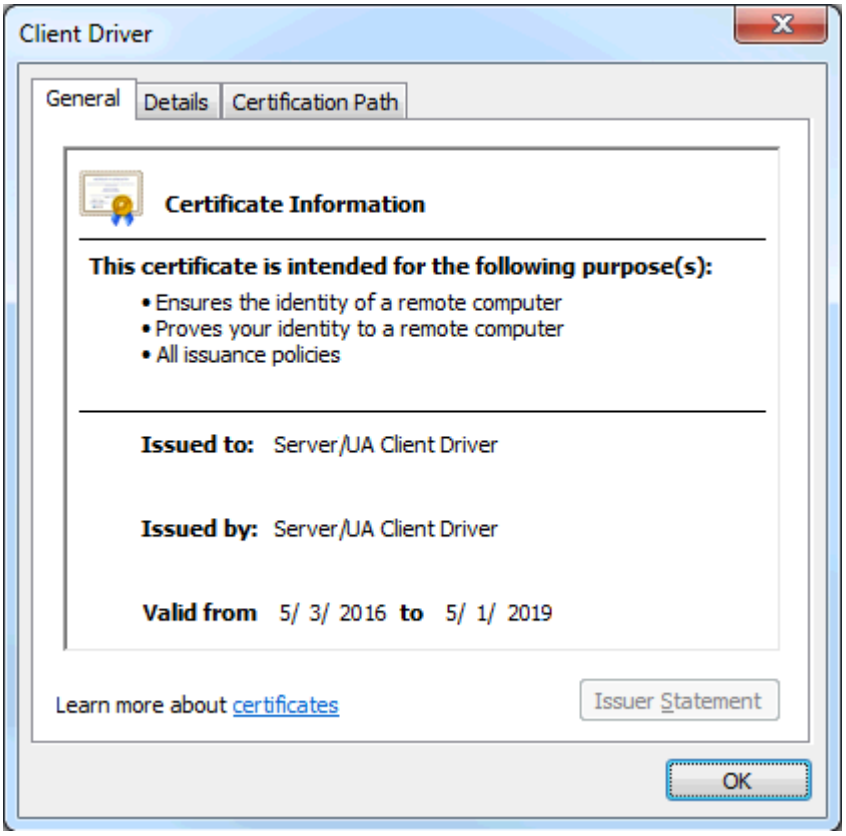
- rsa-sha256

Zertifikatanzeige

Das Dialogfenster sollte wie folgt aussehen, wenn der Serverzertifikat anzeigt wird:

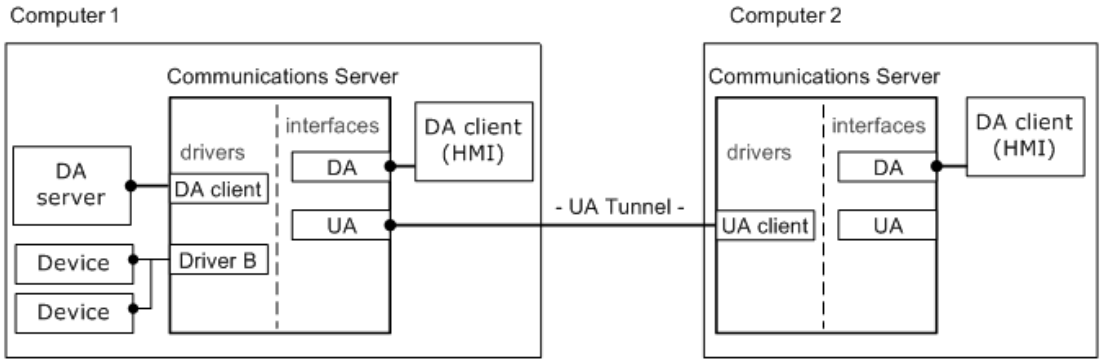


Das Dialogfenster sollte wie folgt aussehen, wenn der Client-Treiber-Zertifikat anzeigt wird:


Client Driver
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• All issuance policies
Issued to: Server/UA Client Driver
Issued by: Server/UA Client Driver
Valid from 5/ 3/ 2016 to 5/ 1/ 2019
Learn more about certificates
Issuer Statement
OK

OPC UA Lernprogramm

Dieses Lernprogramm enthält Anweisungen zur Konfiguration einer sicheren OPC UA-Verbindung zwischen zwei Remote-Computern auf denen der Kommunikationsserver läuft.



Es werden den folgenden Laufzeit-Komponenten benötigt:

- Der Kommunikationsserver mit UA-Serverschnittstelle auf Computer 1.
- Der Kommunikationsserver mit UA-Client-Treiber auf Computer 2.

Hinweis: Der OPC DA-Client-Treiber (in der Abbildung Computer 1) ist eine optionale Komponente, die für die Verbindung zu externen OPC DA-Servern verwendet wird.

Voraussetzungen

Sie müssen folgende Schritte ausführen, bevor Sie fortfahren können:

1. Installieren Sie die Serveranwendung auf dem Client-Computer. Schließen Sie im Dialogfenster Funktionen auswählen den OPC UA-Client-Treiber (unter **Kommunikationstreiber**) ein.
2. Installieren Sie die Serveranwendung auf dem Servercomputer. Da die UA-Funktionalität eingeschlossen ist, müssen während der Installation keine weiteren Funktionen ausgewählt werden.

Hinweis: Bestimmte Anwendungen erfordern möglicherweise, dass jeder Computer als Server sowie als Client agiert. Sollte dies der Fall sein, installieren Sie den OPC UA-Client-Treiber auf jedem Computer, der remote auf Elemente zugreifen muss.

Sicherheit

Anstatt sich, was die Sicherheit der Anwendungen betrifft, auf das Betriebssystem des Computer zu verlassen, verwendet OPC UA die X.509-Authentifizierungstechnologie. Diese Technologie besteht aus einem Satz öffentlicher und privater Schlüssel für jede Entität, die Vertrauen herstellen möchte. Der private Schlüssel ist geschützt und der öffentliche Schlüssel wird für die Verteilung in ein Zertifikat platziert. Der Client und der Server müssen Zertifikate austauschen, um eine sichere Verbindung herzustellen. Dieser Austausch muss nur einmal während der Gültigkeitsdauer des Zertifikats stattfinden.

Der manuelle Austausch besteht aus dem Export und Import einer Zertifikatdatei auf jedem Computer. Es muss ein Wechselmedium (oder eine andere Form der Dateiübertragung) verwendet werden, damit der Austausch stattfinden kann. Der manuelle Prozess erlaubt es auch, dass Zertifikate zwischen Clients und Servern, die den Umfang dieser Anwendung übersteigen, ausgetauscht werden können.

Ist Sicherheit nicht obligatorisch, kann der Zertifikataustausch übersprungen werden. Die Sicherheitsstufe wird beim Definieren der Serverendpunkte vom Benutzer festgelegt. Wird "Keine" ausgewählt, so werden die Zertifikate nicht für Validierung geprüft. *Weitere Informationen zu unsicheren Verbindungen finden Sie unter Server einrichten*.

Austausch

1. Starten Sie OPC UA Configuration Manager auf dem Servercomputer durch Rechtsklick auf das Symbol **Verwaltung** in der Taskleiste. Wählen Sie **OPC UA Konfiguration** aus.

2. Wählen Sie anschließend **Instanzzertifikat** aus. Klicken Sie unter der Gruppe **Server** auf **Serverzertifikat exportieren**. Wählen Sie einen Speicherort, auf den leicht zugegriffen werden kann, für die Zertifikatdatei aus. Der Standarddateiname kann, falls gewünscht, geändert werden.
3. Kopieren Sie die Serverzertifikatdatei manuell vom Servercomputer und verschieben Sie sie auf den Client-Computer.
4. Starten Sie als Nächstes OPC UA Configuration Manager auf dem Client-Computer.
5. Wählen Sie die Registerkarte **Vertrauenswürdige Server** aus, und klicken Sie anschließend auf **Importieren**.
6. Suchen Sie nach der Serverzertifikatdatei und klicken Sie auf **Öffnen**. Das Serverzertifikat sollte im Fenster **Vertrauenswürdige Server** angezeigt werden und kann anhand der URI identifiziert werden.
7. Wählen Sie anschließend **Instanzzertifikat** aus. Wählen Sie unter der Gruppe **Client-Treiber** die Option **Client-Treiber-Zertifikat exportieren** aus. Wählen Sie einen Speicherort, auf den leicht zugegriffen werden kann, für die Zertifikatdatei aus. Der Standarddateiname kann, falls gewünscht, geändert werden.
8. Kopieren Sie die Client-Zertifikatdatei manuell vom Client-Computer und geben Sie sie an den Servercomputer zurück.
9. Starten Sie als Nächstes OPC UA Configuration Manager auf dem Client-Computer.
10. Wählen Sie die Registerkarte **Vertrauenswürdige Clients** aus, und klicken Sie anschließend auf **Importieren**.
11. Suchen Sie nach der Client-Zertifikatdatei und klicken Sie auf **Öffnen**. Das Client-Zertifikat sollte im Fenster **Vertrauenswürdige Clients** angezeigt werden. Es kann anhand seiner URI identifiziert werden.

Server einrichten

Endpunkte

Damit ein OPC UA-Client eine Verbindung zu einem OPC UA-Server herstellen kann, muss der Client den Serverstandort und die Sicherheitsanforderungen kennen. In seiner komplexen Form verwendet der Client einen Speicherort und eine Portnummer (Ermittlungsendpunkt genannt), um Informationen zum Server zu ermitteln. Im Gegenzug gibt der Server alle konfigurierten Endpunkte zusammen mit den Sicherheitsanforderungen, die dem Client zur Verfügung stehen, zurück. Um den Prozess zu vereinfachen, können sich der Ermittlungsendpunkt und der Serverendpunkt am gleichen Speicherort (wie es bei dieser Serveranwendung der Fall ist) befinden.

Während der Server-Anwendungsinstallation wird ein anfänglicher Endpunkt für lokale Verbindungen erstellt. Die Konfiguration muss geringfügig geändert werden, damit Remote-Clients den Server ermitteln und eine Verbindung zu ihm herstellen können. Am Server müssen keine Änderungen vorgenommen werden, damit er lokale Verbindungen herstellen kann. Weitere Informationen zum Hinzufügen und Ändern von vorhandenen Endpunkten finden Sie in den nachfolgenden Anweisungen.

1. Starten Sie OPC UA Configuration Manager durch Rechtsklick auf das Symbol **Verwaltung** in der Taskleiste. Wählen Sie **OPC UA Konfiguration** aus.
2. Klicken Sie auf **Serverendpunkte** und wählen Sie anschließend den Standard-Endpunkt, der bei der Installation für nicht lokale Verbindungen erstellt wurde, aus.
3. Klicken Sie auf **Bearbeiten**.
   Hinweis: Schreiben Sie sich die Portnummer auf, so dass Sie sie später zu Ihrer Firewall hinzufügen können.
4. Ändern Sie ggf. die Einstellungen für **Sicherheitsrichtlinien**. Da es sich hierbei um Servereinstellungen handelt, lässt dieser spezifische Endpunkt alle Verbindungen mit aktivierten Richtlinien zu. Das bedeutet, das der Standard-Endpunkt nur sichere Verbindungen, die Signatur und Verschlüsselung verwenden, zulässt. Wählen Sie "Keine" aus, wenn Sicherheit nicht erforderlich ist. Benutzer, die diese Auswahl treffen, möchten die Sicherheitsrichtlinien möglicherweise vollständig deaktivieren.
5. Klicken Sie, sobald die Richtlinien entsprechend angepasst wurden, auf **OK**.
6. Um den Endpunkt zu aktivieren, wählen Sie ihn in der Liste aus, und klicken Sie auf **Aktivieren**.

7. Wenden Sie die Änderungen auf die Server-Laufzeit an, indem Sie mit der rechten Maustaste auf das Symbol **Verwaltung** in der Taskliste klicken und dann **Neu initialisieren** auswählen. Wird der Server nicht ausgeführt, klicken Sie mit der rechten Maustaste auf das Symbol **Verwaltung** und wählen Sie anschließend **Laufzeitdienst starten** aus.

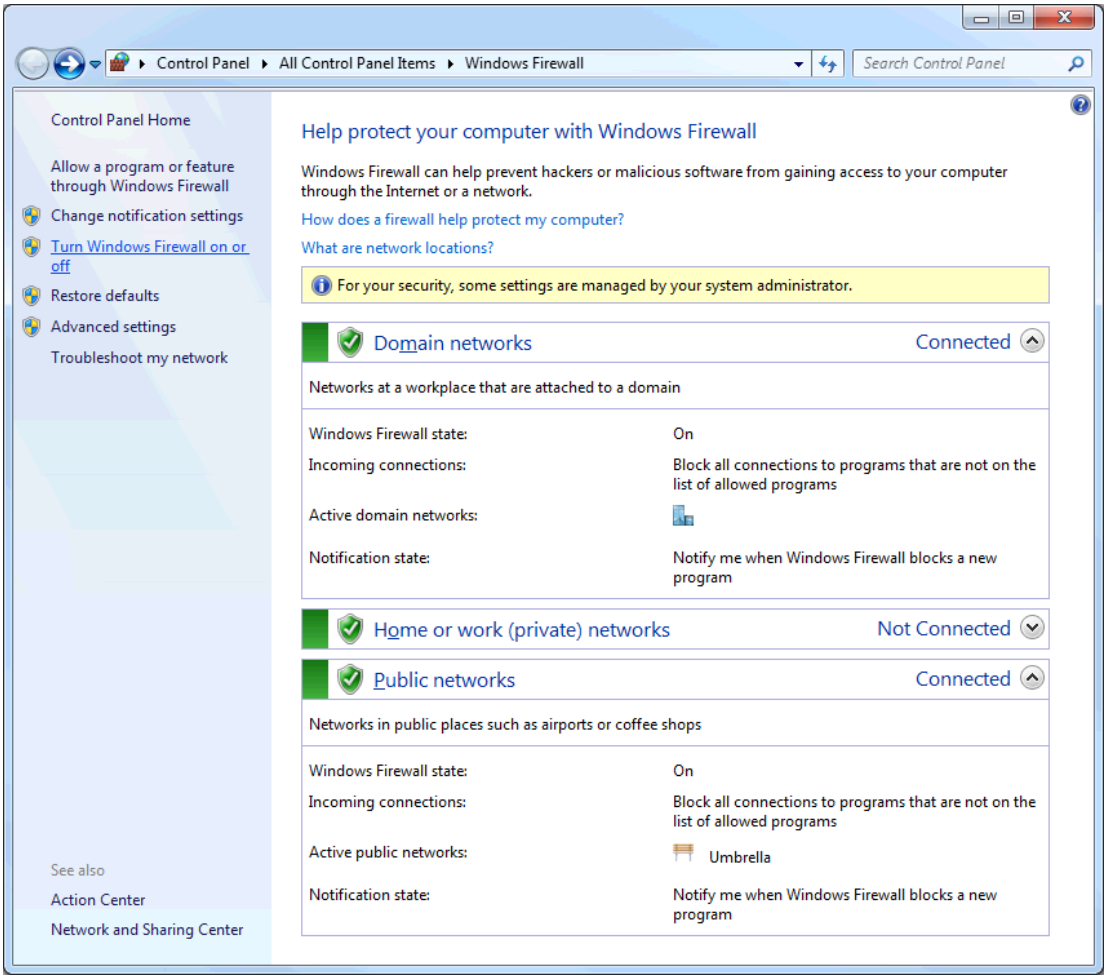
Ermittlungsdienst (Optional)
Benutzer, die sich mit OPC DA auskennen, sind möglicherweise mit OPCEnum vertraut, einer Anwendung, die lokal auf dem übermittelnden Computer ausgeführt wird und vorhandene OPC DA-Server für Clients, die eine Remoteverbindung herstellen, verfügbar macht. Der Client muss lediglich den Speicherort des übermittelnden Computers im Netzwerk kennen.

Es wurde ein Dienst erstellt, der es erlaubt, dass OPC UA-Servern an einem "bekannten" Speicherort ermittelt werden können, um eine ähnliche Benutzerfreundlichkeit zu bieten und dennoch plattformunabhängig zu sein. Bei diesem Dienst handelt es sich um den **lokalen Ermittlungsdienst (Local Discovery Service, LDS)**, der auf jedem Computer, der einen OPC UA-Server ausführt, installiert sein sollte (genau wie OPCEnum mit den meisten klassischen OPC-Servern installiert ist). Da die Entwicklung und Implementierung des LDS noch nicht so weit fortgeschritten ist wie OPC UA, variiert die tatsächliche Verwendung dieses Dienstes.
Hinweis: Diese Serveranwendung stellt keinen LDS bereit, kann jedoch so konfiguriert werden, dass sie mit einem LDS registriert wird.

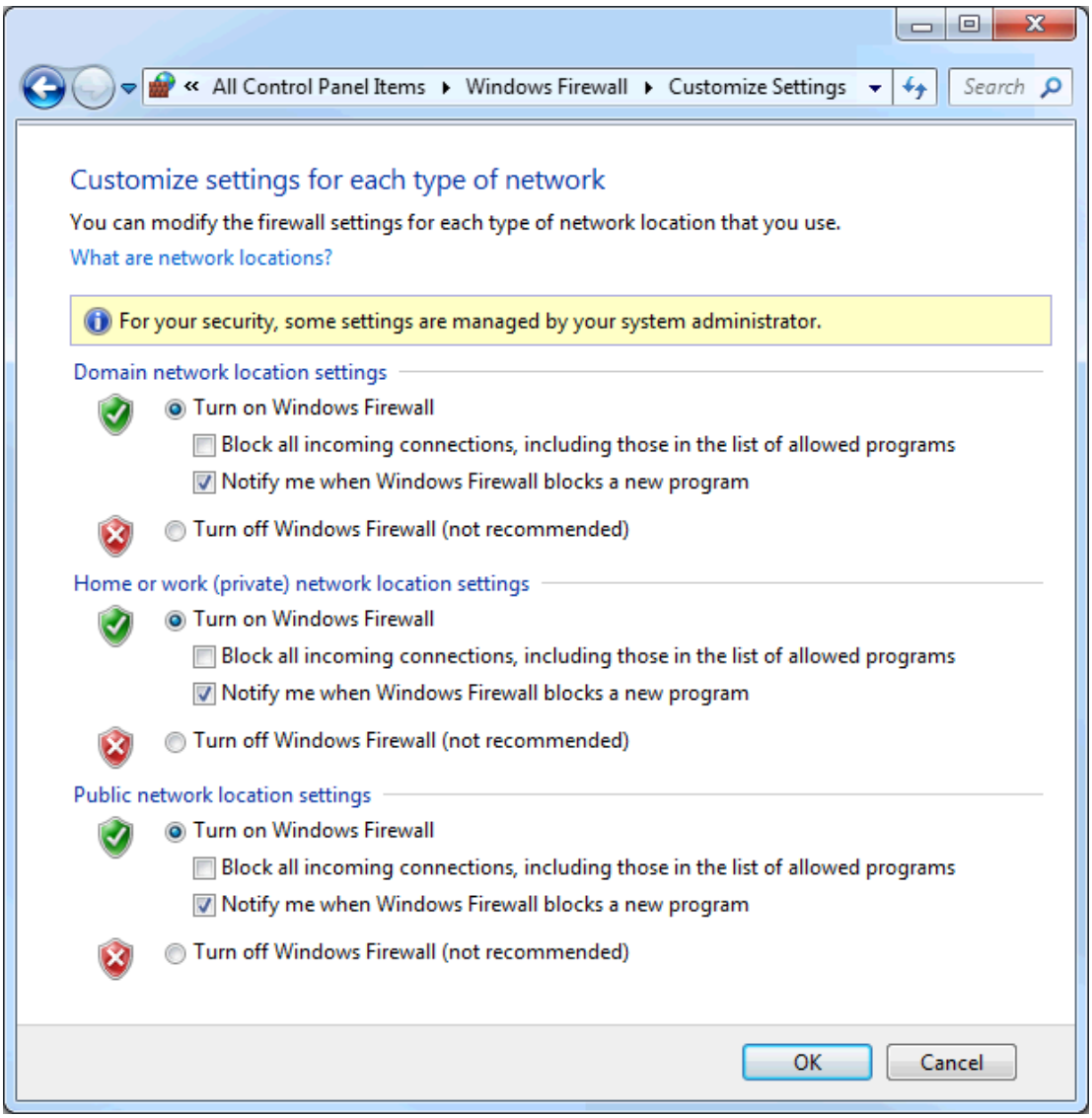
Firewall
Die Firewall schützt vor nicht erwartetem, eingehendem Datenverkehr (d.h. nicht angeforderter Datenverkehr) oder Datenverkehr, der nicht den Ausnahmen (erwarteter Datenverkehr), die für die Firewall festgelegt wurden, entspricht. Da OPC UA keine Callbacks erfordert, müssen Ausnahmen nur für den Servercomputer festgelegt werden.

Befolgen Sie die nachfolgenden Anweisungen auf dem Servercomputer, um eine Ausnahme hinzuzufügen.

1. Starten Sie die Windows-Firewall, indem Sie **Start** | **Ausführen** auswählen. Geben Sie **firewall.cpl** ein.

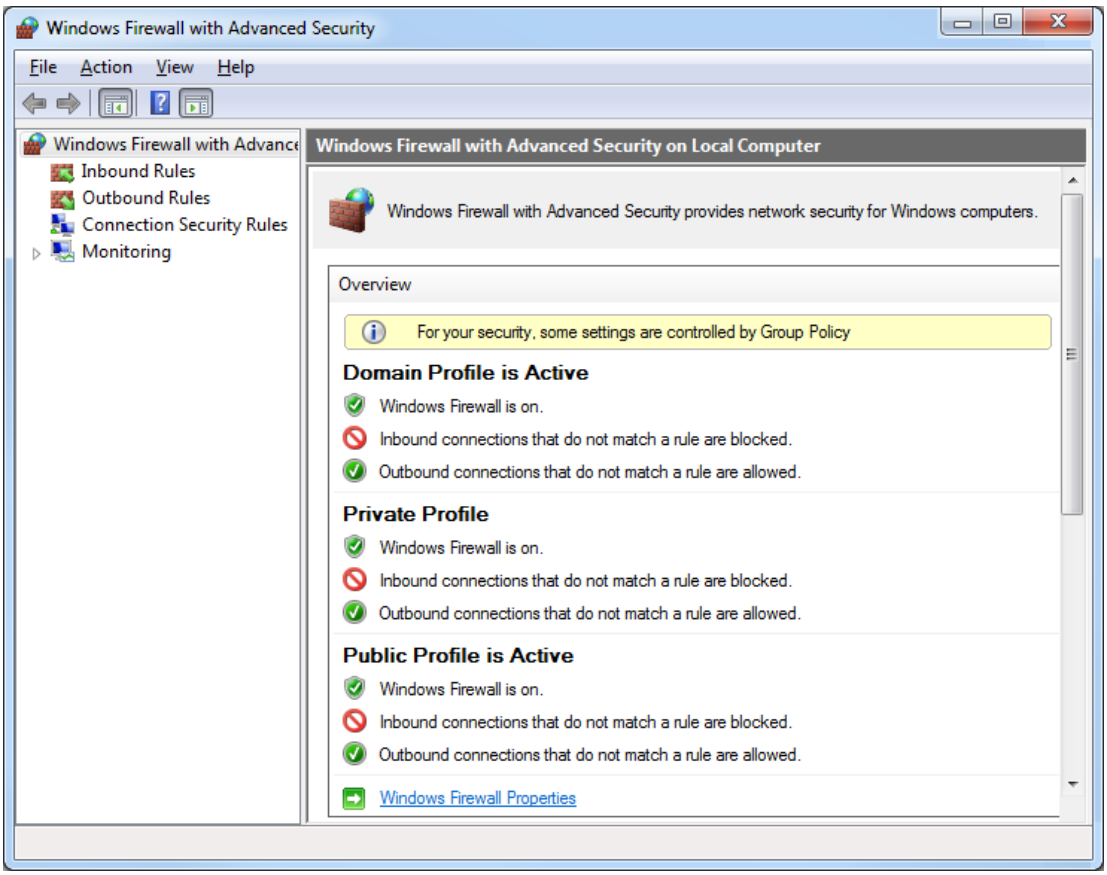

Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
For your security, some settings are managed by your system administrator.
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active domain networks:
Notification state: Notify me when Windows Firewall blocks a new program
Home or work (private) networks
Not Connected
Public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active public networks: Umbrella
Notification state: Notify me when Windows Firewall blocks a new program

2. Klicken Sie auf **Windows-Firewall ein- oder ausschalten**.



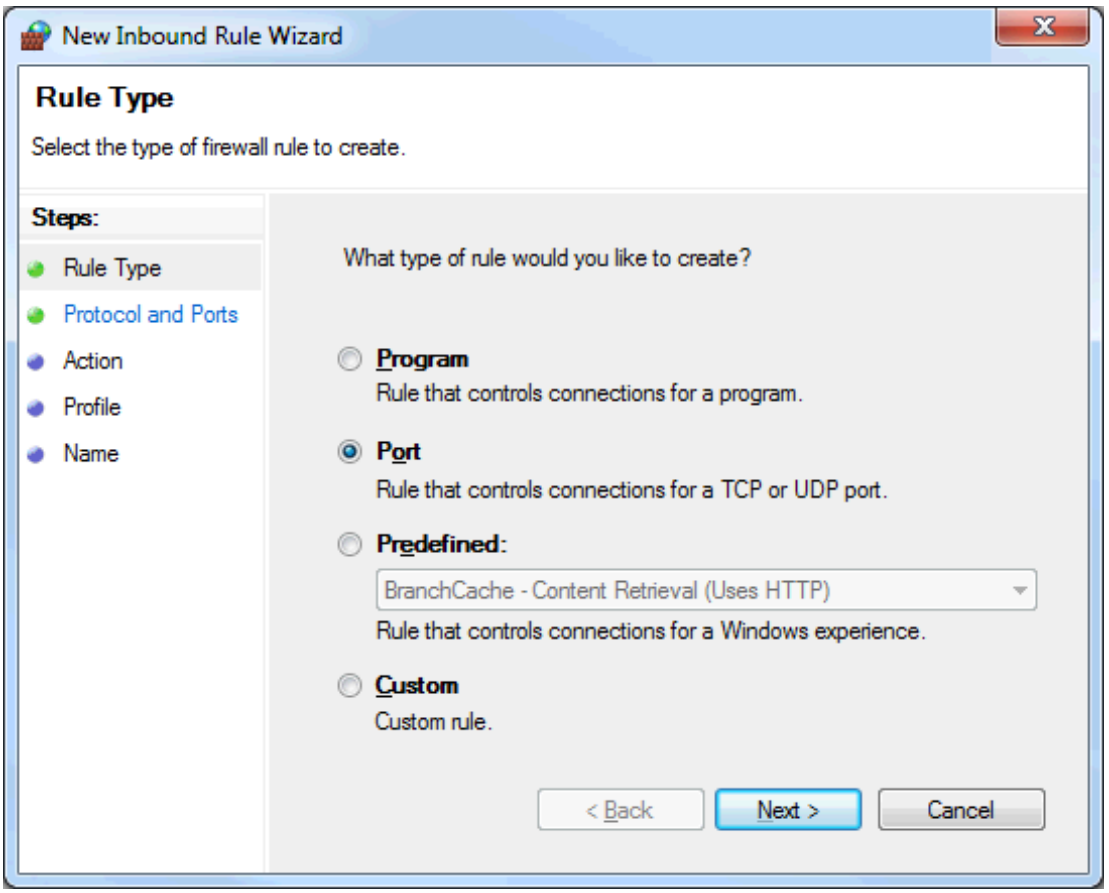
3. Stellen Sie sicher, dass die Firewall aktiviert ist.

4. Klicken Sie auf **Erweiterte Einstellungen**.

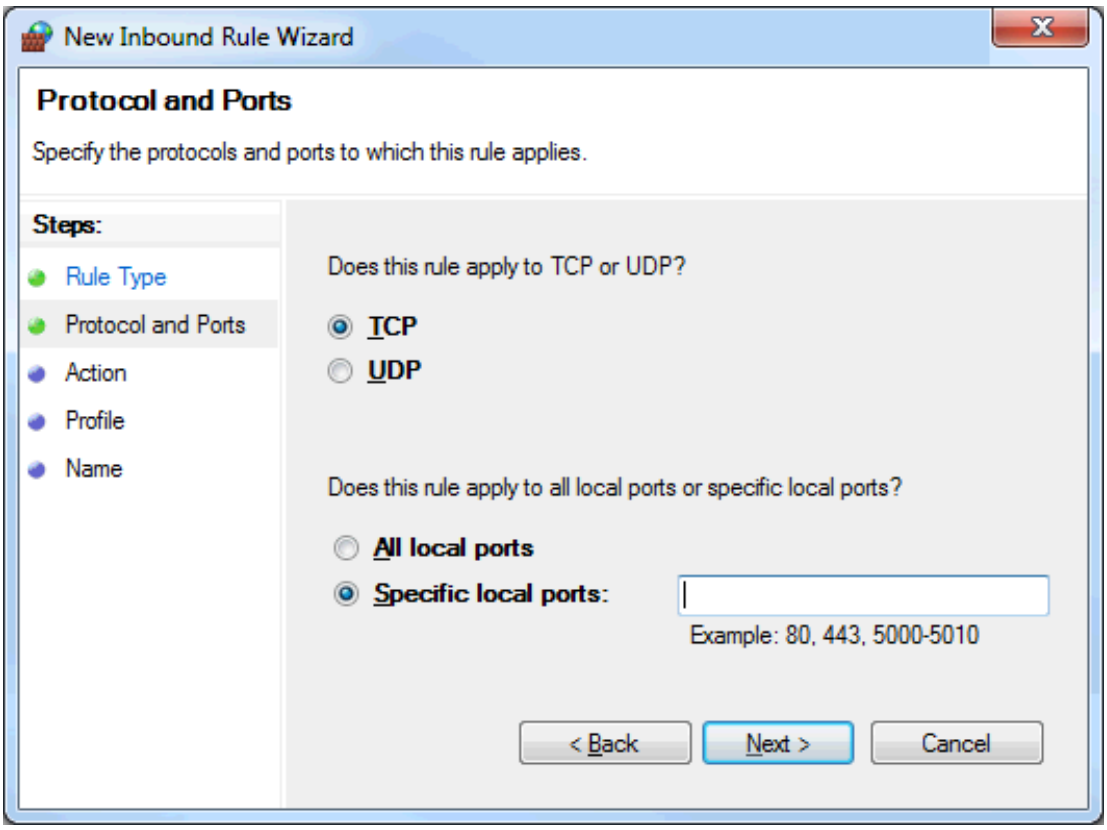


5. Klicken Sie auf **Windows-Firewalleigenschaften**.
6. Wählen Sie im linken Bereich **Eingehende Regeln** aus.
7. Wählen Sie **Neue Regel...** im rechten Aktionsbereich.

8. Wählen Sie **Port** als Regeltyp aus.



9. Wählen Sie **Bestimmte lokale Ports** aus.



10. Geben Sie den dem Endpunkt zugewiesenen UA-Endpunkt ein.
11. Klicken Sie auf **Weiter**.
12. Vergewissern Sie sich, dass das richtige Protokoll ausgewählt ist. Die Standardeinstellung ist TCP.
13. Klicken Sie auf **OK**.
14. Wurden dem Server mehrere Endpunkte zugewiesen, fügen Sie diese jetzt hinzu. Wenn Sie fertig sind, klicken Sie auf **OK**.

Client einrichten

OPC UA Client-Treiber-Kanal

Der Kanal-Assistent wird verwendet, um den OPC UA-Server zu suchen und zu identifizieren, Sitzungs-Timeouts zu konfigurieren und ggf. Benutzerinformationen zur Verfügung zu stellen. Informationen zum Hinzufügen eines UA Client-Kanals finden Sie in den nachfolgenden Anweisungen.

1. Beginnen Sie, indem Sie mit der rechten Maustaste auf das Symbol **Verwaltung** in der Taskleiste klicken, um die Konfiguration zu starten. Wählen Sie **Konfiguration** aus.
2. Wählen Sie **Bearbeiten** | **Konnektivität** | **Neuer Kanal** aus.
3. Wählen Sie im Dropdown-Menü **Wählen Sie den Typ des zu erstellenden Kanals aus** die Option **OPC UA Client** aus und klicken Sie auf **Weiter**.
4. Geben Sie unter **Geben Sie die Identität dieses Objekts an** den Namen für den Kanal an, und klicken Sie anschließend auf **Weiter**.
5. Behalten Sie die Standardeinstellungen in **Schreiboptimierungen** bei, und klicken Sie auf **Weiter**.
6. Geben Sie in **UA Server** manuell die Endpunkt-URL des Servers in das Feld **Endpunkt-URL** ein.

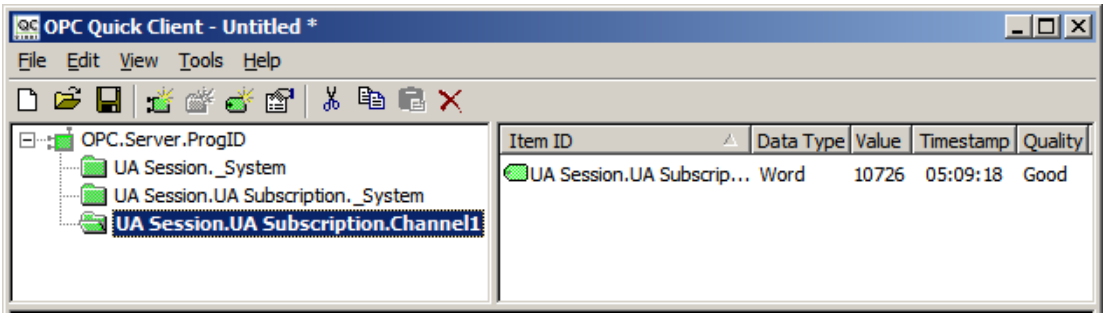
7. Alternativ können Sie auf das Symbol zum Durchsuchen (...) klicken und die Endpunkt-URL auf dem Computer suchen.
    a. Stellen Sie sicher, dass der Parameter **Ermittlungs-URL verwenden** deaktiviert ist.
    b. Geben Sie im Parameter **Ermittlungs-Port** die Endpunkt-Portnummer, die auf dem Servercomputer erstellt wurde, ein. Die Standard-Portnummer sollte bereits zugewiesen sein und mit dem Standard-Endpunkt übereinstimmen.
    Hinweis: Port 4840 wird immer vom Browser gescannt. Folglich ist es bei der Verwendung eines Ermittlungsservers nicht notwendig, die richtige Portnummer in dieses Feld einzugeben.
    c. Wurde die Portnummer geändert, klicken Sie auf **Aktualisieren**.
    d. Suchen Sie nach dem Servercomputer. Endpunkte, die "localhost" zugewiesen sind, werden nur unter dem Zweig **Lokaler Rechner** gefunden.
    e. Erweitern Sie den Computer, um eine Liste der verfügbaren Server anzuzeigen, und erweitern Sie anschließend die Server und wählen Sie den richtigen Endpunkt aus.
    f. Wenn Sie diesen Endpunkt weiterhin zum Ermitteln von UA-Servern verwenden möchten, aktivieren Sie **Ermittlungs-URL verwenden im** Parameter **Ermittlung** oben im Dialogfenster. Hierbei handelt es sich um eine globale Änderung, die sich auf alle anderen UA-Client-Treiber auswirkt.
    g. Klicken Sie auf **OK**. Die Endpunktinformationen werden auf der Seite "UA Server" angezeigt. Klicken Sie auf **Weiter**.
8. Behalten Sie die Standardeinstellungen für **UA Sitzung** bei, indem Sie auf **Weiter** klicken. Falls gewünscht, können diese Einstellungen zu einem späteren Zeitpunkt optimiert werden.
9. Lassen Sie den Benutzernamen und das Passwort unter **Authentifizierung** leer, indem Sie auf **Weiter** klicken. Diese Angaben können, falls gewünscht, geändert werden.
10. Zeigen Sie die Informationen unter **Zusammenfassung** an, und klicken Sie auf **Beenden**.

OPC UA Client-Gerät
Der Geräte-Assistent hilft Benutzern dabei, ein Abonnement einzurichten und bietet eine Möglichkeit, Elemente zu suchen und diese vom OPC UA Server zu importieren. Alle Elemente im Gerät werden entsprechend der angegebene Einstellungen aktualisiert. Mehrere Geräte können zum selben Kanal hinzugefügt werden, um unterschiedliche Aktualisierungsintervalle und -modus zu ermöglichen. Informationen zum Hinzufügen eines UA Client-Geräts finden Sie in den nachfolgenden Anweisungen.

1. Wählen Sie zunächst den neuen Kanal aus und klicken Sie auf **Bearbeiten** | **Konnektivität** | **Neues Gerät**.
2. Geben Sie unter **Name** einen Namen für das OPC UA Client-Gerät ein und klicken Sie anschließend auf **Weiter**.
3. Behalten Sie die Standardeinstellungen bei und fahren Sie fort, indem Sie auf **Weiter** klicken. Falls gewünscht, können diese Einstellungen zu einem späteren Zeitpunkt optimiert werden.
4. Klicken Sie unter **Importieren** auf **Importelemente auswählen**. Die verfügbaren Elemente für den Server sollten im Browserfenster angezeigt werden. Falls nicht, ist die Sicherheitskonfiguration möglicherweise falsch. Weitere Informationen finden Sie unter Tipps zur Problembehandlung.
5. Wählen Sie die gewünschten Elemente aus und klicken Sie auf **Elemente hinzufügen** oder **Zweige hinzufügen**, um die Elemente in den Client zu importieren. Klicken Sie, sobald alle Elemente importiert wurden, auf **OK** gefolgt von **Weiter**.
6. Zeigen Sie die Informationen unter **Zusammenfassung** an, und klicken Sie auf **Beenden**. Die importierten Elemente werden unterhalb des Geräts eingefüllt und der Kanal des Servers und die Gerätenamen werden als Gruppen verwendet.

Überprüfung
Die im OPC UA Client hinzugefügten Elemente können jetzt von einem OPC DA Client gesucht werden. Folgen Sie den nachstehenden Anweisungen, für eine einfache Überprüfung.

1. Wählen Sie **Tools** | **OPC Quick Client starten** aus. Es wird eine Verbindung zum lokalen OPC DA Server hergestellt und die Ansicht wird mit Elementen gefüllt.



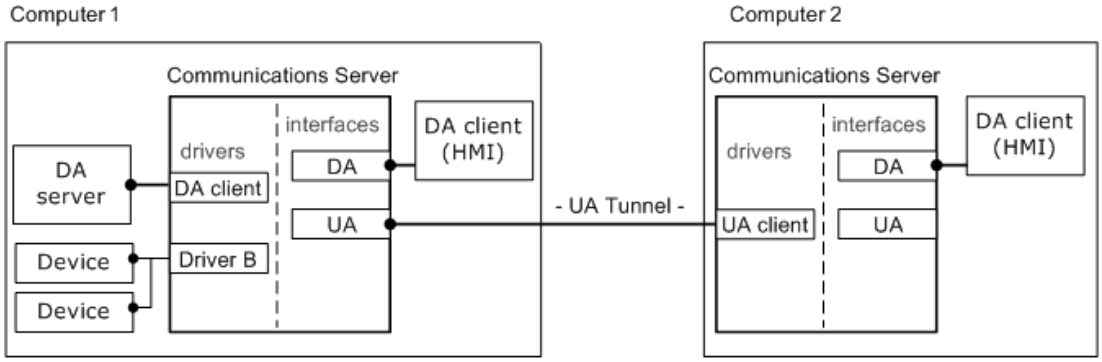
2. Suchen Sie nach den Elementen im OPC UA Kanal. Verifizieren Sie anschließend, dass die Datenqualität gut ist und die Werte aktualisiert werden.

Verbindungsbeispiele

Der OPC UA Tunnel ist kein eigentliches Produkt, sondern eine Remoteverbindungs-Lösung, die aus vorhandenen verfügbaren Komponenten erstellt wurde. Auf der Serverseite des Tunnels ist der OPC UA Server eine Benutzeroberfläche, die neben OPC DA im gesamten Kommunikationsserver-Produkt gepackt ist. Auf der Clientseite des Tunnels ist der OPC UA Client-Treiber ein Treiber-Plugin, das zusammen mit anderen Gerätekanälen hinzugefügt werden kann. OPC UA Configuration Manager ist ein Tool, das die Verwaltung von vertrauenswürdigen Zertifikaten und UA Server-Endpunkten ermöglicht. Der DA Client-Treiber ist ein zusätzliches Treiber-Plugin, welches die UA-Tunnellösung weiter verbessert. Da es sich beim Kommunikationsserver um einen "Server" handelt, bietet dieser Treiber Konnektivität zu anderen OPC DA-Servern.

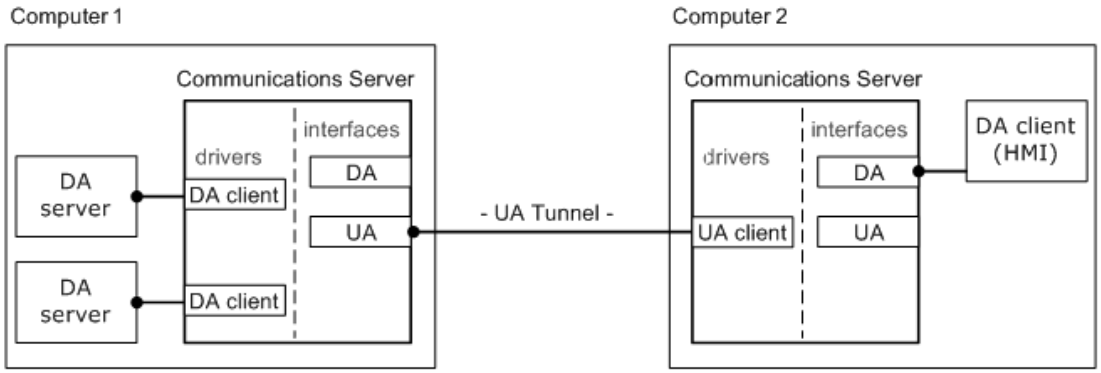
Daten aus der Fabrik für Remote-Clients bereitstellen

Der Kommunikationsserver stellt Daten für lokale OPC DA-Clients bereit sowie für Remote-OPC DA-Clients. Die UA Tunnel-Lösung bietet die sichere Remote-Verbindung



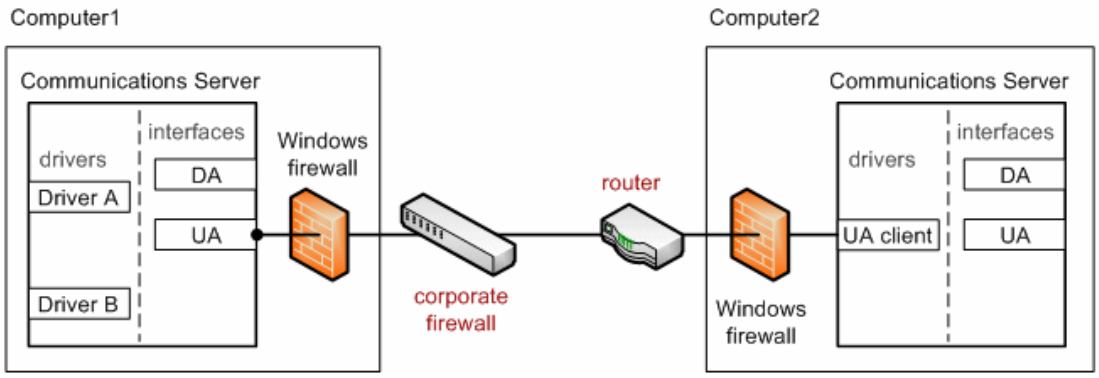
Sichere Aggregatdaten von externen DA-Servern bereitstellen

Der Kommunikationsserver verwendet den OPC DA Client-Treiber, um eine Verbindung zu OPC DA-Servern herzustellen. Anschließend werden Aggregatdaten sicher für Remote-OPC DA-Clients bereitgestellt.



Beispiel: Firewall und Routing-Architektur

Es ist wahrscheinlich, dass Benutzer eine Port-Ausnahme (z.B. UA-Server-Endpunkt-Port) für die Windows-Firewall auf Computer 1 erlauben müssen, zusätzlich zum Öffnen eines Ports in der Unternehmensfirewall. Für die Windows-Firewall auf Computer 2 sollten keine Änderungen erforderlich sein. Der Router auf der Client-Seite der Verbindung erfordert jedoch möglicherweise, dass ein Port geöffnet oder eine Portweiterleitungs-Option aktiviert wird.


Computer1
Communications Server
drivers
interfaces
DA
Driver A
UA
Driver B
Windows firewall
corporate firewall
router
Computer2
Communications Server
drivers
interfaces
DA
UA client
UA
Windows firewall

Tipps zur Problembehandlung

Klicken Sie auf den Link für eine Beschreibung des Problems.

Tipps zur Problembehandlung

Beim Versuch, Elemente in das Dialogfenster "Geräteeigenschaften" zu importieren, kann keine Verbindung zum UA Server hergestellt werden
Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen
Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird
Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden
Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort)
Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden
Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll

Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen

Mögliche Ursache:

1. Der im Feld "Ermittlungs-Port" aufgelistete Endpunkt-Port ist falsch.
2. Der Endpunkt ist auf dem UA Server nicht aktiviert.
3. Die UA Server-Benutzeroberfläche ist in den Projekteigenschaften deaktiviert.
4. Der UA Server und der Endpunkt sind aktiviert und richtig, Änderungen wurden jedoch nicht in der Server-Laufzeit gespeichert.

Lösung:

1. Bestätigen Sie den im UA Server definierten Endpunkt und geben Sie den richtigen Port in das Feld "Ermittlungs-Port" ein. Aktualisieren Sie anschließend die Ansicht.
2. Starten Sie den OPC UA Configuration Manager auf dem UA Server-Computer, um sich zu vergewissern, dass der Endpunkt aktiviert ist.
3. Starten Sie die Serverkonfiguration. Prüfen Sie unter **Bearbeiten**| **Projekteigenschaften** die Eigenschaftsgruppe **OPC UA** hinsichtlich der Einstellungen für die Serverschnittstelle.
4. Stellen Sie sicher, dass **Aktivieren** auf **Ja** festgelegt ist.
5. Speichern Sie das Projekt aus der Konfiguration und klicken Sie auf **Ja**, wenn Sie dazu aufgefordert werden, die Änderungen in der Laufzeit zu speichern.

Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird

Mögliche Ursache:

Der Zielcomputer wurde nicht zur Netzwerk-Domäne hinzugefügt. Der Zielcomputer befindet sich möglicherweise lediglich in einer Arbeitsgruppe und nicht in einer Domäne.

Lösung:

Bestätigen Sie die Endpunkt-URL vom UA Configuration Manager auf dem UA Servercomputer. Geben Sie anschließend die Endpunkt-URL im UA Client-Treiber-Kanal manuell ein.

Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden

Mögliche Ursache:

1. Die Unternehmensfirewall auf der Client-Seite der Verbindung erlaubt möglicherweise nur Verbindungen über einen einzelnen Port (wie z.B. 8080).
2. Der serverseitige Router/Switch muss so konfiguriert werden, dass eingehende Client-Anforderungen an den UA Server-Computer weitergeleitet werden.
3. Die Windows-Firewall blockiert die eingehende Anforderung vom UA-Client.

Lösung:

1. Öffnen Sie einen Port in der Unternehmensfirewall für die UA-Tunnelverbindung. Alternativ können Sie den Endpunkt-Port auf dem UA Server zurücksetzen, so dass er dem Port entspricht, den die Unternehmensfirewall erlaubt.
2. Konfigurieren Sie Portweiterleitung im Router. Die URL des UA-Clients verwendet in diesem Fall die IP-Adresse des Routers mit der Portnummer, die für den UA Server-Endpunkt (die für die Portweiterleitung verwendete Portnummer) verwendet wird.
3. Fügen Sie eine Ausnahme für den Endpunkt-Port zur Windows-Firewall hinzu.

Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort)

Mögliche Ursache:

Der Client-Sitzungen-Parameter für den UA Server, **Anonyme Anmeldung zulassen** wurde auf **Nein** festgelegt.

Lösung:

Starten Sie die Serverkonfiguration und wählen Sie ein Projekt in der Baumansicht aus. Prüfen Sie unter **Bearbeiten** | **Eigenschaften** die OPC UA Eigenschaftsgruppe hinsichtlich der Einstellungen für Client-Sitzungen und bestätig Sie, dass **Anonyme Anmeldung zulassen** auf **Ja** festgelegt ist.

Hinweis:

Ist Authentifizierung erforderlich, greifen Sie über die Serververwaltung (in der Taskleiste) auf den Benutzermanager zu, um den Benutzernamen und das Passwort festzulegen.

Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden

Mögliche Ursache:

Die Standardeinstellung des Routers ist möglicherweise, nicht auf das Pingen zu reagieren.

Lösung:

Aktivieren Sie auf der Serverseite des Routers, dass auf das Pingen reagiert wird. Deaktivieren Sie diese Einstellung, nachdem erfolgreich auf das Pingen reagiert wurde.

Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll

Mögliche Ursache:

OPC UA Serverdiagnose ist nicht aktiviert.

Lösung:

Starten Sie die Serverkonfiguration und wählen Sie **Projekt** in der Baumansicht aus. Wählen Sie **Bearbeiten** | **Projekteigenschaften**. Suchen Sie auf der Registerkarte UA nach der Serverschnittstelle und bestätigen Sie, dass "Protokolldiagnose" auf "Ja" festgelegt ist.

Ereignisprotokollmeldungen

Die folgenden Informationen betreffen Meldungen, die im Fensterbereich Ereignisprotokoll in der Hauptbenutzeroberfläche angezeigt werden. Informationen zum Filtern und Sortieren der Detailansicht Ereignisprotokoll finden Sie in der OPC-Serverhilfe. In der Serverhilfe sind viele allgemeine Meldungen enthalten, die also auch gesucht werden sollten. Im Allgemeinen werden die Art der Meldung (Information, Warnung) sowie Fehlerbehebungsinformationen bereitgestellt (sofern möglich).

Konto '<Name>' hat keine Berechtigung zum Ausführen der Anwendung.

Fehlertyp:
Fehler

Mögliche Ursache:
Der derzeit angemeldete Benutzer verfügt nicht über ausreichende Berechtigungen.

Mögliche Lösung:

1. Melden Sie sich mit einem Administrator-Konto an.
2. Wenden Sie sich an den Systemadministrator, um Berechtigungen zu verifizieren oder zu aktualisieren.
3. Verifizieren oder korrigieren Sie die Zugriffsrechte für das Anwendungsdatenverzeichnis für diese Anwendung.

Siehe auch:
Anwendungsdaten (in der Server-Hilfe) und der Abschnitt "Application Data User Permissions" des englischen Handbuchs Secure Deployment Guide

Das Zertifikat des UA Server wurde erneut ausgestellt. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen.

Fehlertyp:
Sicherheit

Das Zertifikat des UA Client Treibers wurde erneut ausgestellt. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann.

Fehlertyp:
Sicherheit

Das UA Client Zertifikat '<Client-Name>' wurde zurückgewiesen. Der Server kann keine Verbindungen von dem Client annehmen.

Fehlertyp:
Sicherheit

Das UA Client Zertifikat '<Client-Name>' wurde als vertrauenswürdig eingestuft. Der Server kann Verbindungen von dem Client annehmen.

Fehlertyp:
Sicherheit

Das UA Server Zertifikat '<Servername>' wurde zurückgewiesen. Der UA Client Treiber kann keine Verbindung zum Server herstellen.

Fehlertyp:
Sicherheit

Das UA Server Zertifikat '<Servername>' wurde als vertrauenswürdig eingestuft. Der UA Client Treiber kann eine Verbindung zum Server herstellen.

Fehlertyp:
Sicherheit

Das UA Server Zertifikat '<Servername>' wurde zur Liste der vertrauenswürdigen Server hinzugefügt. Der UA Client Treiber kann jetzt eine Verbindung zum Server herstellen.

Fehlertyp:
Sicherheit

Das UA Client Zertifikat '<Client-Name>' wurde zur Liste der vertrauenswürdigen Clients hinzugefügt. Der UA Server kann jetzt Verbindungen vom Client annehmen.

Fehlertyp:
Sicherheit

Das UA Client Zertifikat '<Client-Name>' wurde aus der Liste der vertrauenswürdigen Clients entfernt. Der UA Server kann keine Verbindungen vom Client annehmen.

Fehlertyp:
Sicherheit

Das UA Server Zertifikat '<Servername>' wurde aus der Liste der vertrauenswürdigen Server entfernt. Der UA Client Treiber kann keine Verbindung zum Server herstellen.

Fehlertyp:
Sicherheit

Der Endpunkt '<URL>' wurde zum UA Server hinzugefügt.

Fehlertyp:
Sicherheit

Der Endpunkt '<URL>' wurde vom UA Server entfernt.

Fehlertyp:
Sicherheit

Der UA Discovery Server '<Servername>' wurde hinzugefügt. Die UA Server Endpunkte können jetzt mit diesem UA Discovery Server registriert werden.

Fehlertyp:
Sicherheit

Der UA Discovery Server '<Servername>' wurde entfernt. Die UA Server Endpunkte können nicht länger mit diesem UA Discovery Server registriert werden.

Fehlertyp:
Sicherheit

Der Endpunkt '<URL>' wurde deaktiviert.

Fehlertyp:
Sicherheit

Das Zertifikat des UA Client Treibers wurde importiert. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann.

Fehlertyp:
Sicherheit

Das Zertifikat des UA Server wurde importiert. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen.

Fehlertyp:
Sicherheit

Der Endpunkt '<URL>' wurde aktiviert.

Fehlertyp:
Sicherheit

Vertrauenswürdigen Client hinzufügen

Das UA Client-Zertifikat '<Zertifikatname>' wurde zu den vertrauenswürdigen Clients hinzugefügt. Der UA Server akzeptiert jetzt Verbindungen vom Client.

Vertrauenswürdigen Client entfernen

Das UA Client-Zertifikat '<Zertifikatname>' wurde aus den vertrauenswürdigen Clients entfernt. Der UA Server akzeptiert keine Verbindungen von diesem Client.

Vertrauenswürdigen Client ablehnen

Das UA Client-Zertifikat '<Zertifikatname>' wurde abgelehnt. Der Server akzeptiert keine Verbindungen von diesem Client.

Vertrauenswürdigem Client vertrauen

Dem UA Client-Zertifikat '<Zertifikatname>' wurde vertraut. Der Server akzeptiert keine Verbindungen vom Client.

Vertrauenswürdigen Server hinzufügen

Das UA Server-Zertifikat '<Zertifikatname>' wurde zu den vertrauenswürdigen Servern hinzugefügt. Der UA Client-Treiber kann jetzt eine Verbindung zum Server herstellen.

Vertrauenswürdigen Server entfernen

Das UA Server-Zertifikat '<Zertifikatname>' wurde aus den vertrauenswürdigen Servern entfernt. Der UA Client-Treiber kann keine Verbindung zum Server herstellen.

Vertrauenswürdigen Server ablehnen

Das UA Server-Zertifikat '<Zertifikatname>' wurde abgelehnt. Der UA Client-Treiber kann keine Verbindung zum Server herstellen.

Vertrauenswürdigem Server vertrauen

Dem UA Server-Zertifikat '<Zertifikatname>' wurde vertraut. Der UA Client-Treiber kann keine Verbindung zum Server herstellen.

Endpunkt hinzufügen

Der Endpunkt '<Endpunktdefinition>' wurde zum UA Server hinzugefügt.

Endpunkt aktivieren

Der Endpunkt '<Endpunktdefinition>' wurde aktiviert.

Endpunkt deaktivieren

Der Endpunkt '<Endpunktdefinition>' wurde deaktiviert.

Endpunkt entfernen

Der Endpunkt '<Endpunktdefinition>' wurde aus dem UA Server entfernt.

Ermittlungsserver hinzufügen

Der Ermittlungsserver '<Zertifikatname>' wurde hinzugefügt. Die UA Server-Endpunkte registrieren sich jetzt mit dem Ermittlungsserver.

Ermittlungsserver entfernen

Der Ermittlungsserver '<Zertifikatname>' wurde entfernt. Die UA Server-Endpunkte registrieren sich nicht länger mit diesem Ermittlungsserver.

Client-Zertifikat erneut ausstellen

Das UA Client-Treiber-Zertifikat wurde erneut ausgestellt. UA Server müssen dem neuen Zertifikat vertrauen, damit der Client-Treiber eine Verbindung herstellen kann.

Serverzertifikat erneut ausstellen

Das UA Server-Zertifikat wurde erneut ausgestellt. Die UA Clients müssen diesem neuen Zertifikat vertrauen, um eine Verbindung herzustellen.

Index

A

Anmeldeinformationen 6
Anonym 6

C

Client-Zertifikat erneut ausstellen 33

D

Das UA Client Zertifikat '<Client-Name>' wurde als vertrauenswürdig eingestuft. Der Server kann Verbindungen von dem Client annehmen. 30
Das UA Client Zertifikat '<Client-Name>' wurde aus der Liste der vertrauenswürdigen Clients entfernt. Der UA Server kann keine Verbindungen vom Client annehmen. 31
Das UA Client Zertifikat '<Client-Name>' wurde zur Liste der vertrauenswürdigen Clients hinzugefügt. Der UA Server kann jetzt Verbindungen vom Client annehmen. 31
Das UA Client Zertifikat '<Client-Name>' wurde zurückgewiesen. Der Server kann keine Verbindungen von dem Client annehmen. 30
Das UA Server Zertifikat '<Servername>' wurde als vertrauenswürdig eingestuft. Der UA Client Treiber kann eine Verbindung zum Server herstellen. 31
Das UA Server Zertifikat '<Servername>' wurde aus der Liste der vertrauenswürdigen Server entfernt. Der UA Client Treiber kann keine Verbindung zum Server herstellen. 31
Das UA Server Zertifikat '<Servername>' wurde zur Liste der vertrauenswürdigen Server hinzugefügt. Der UA Client Treiber kann jetzt eine Verbindung zum Server herstellen. 31
Das UA Server Zertifikat '<Servername>' wurde zurückgewiesen. Der UA Client Treiber kann keine Verbindung zum Server herstellen. 31
Das Zertifikat des UA Client Treibers wurde erneut ausgestellt. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. 30
Das Zertifikat des UA Client Treibers wurde importiert. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. 32
Das Zertifikat des UA Server wurde erneut ausgestellt. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. 30
Das Zertifikat des UA Server wurde importiert. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. 32
Der Endpunkt '<URL>' wurde aktiviert. 32
Der Endpunkt '<URL>' wurde deaktiviert. 32
Der Endpunkt '<URL>' wurde vom UA Server entfernt. 31
Der Endpunkt '<URL>' wurde zum UA Server hinzugefügt. 31
Der UA Discovery Server '<Servername>' wurde entfernt. Die UA Server Endpunkte können nicht länger mit diesem UA Discovery Server registriert werden. 32
Der UA Discovery Server '<Servername>' wurde hinzugefügt. Die UA Server Endpunkte können jetzt mit diesem UA Discovery Server registriert werden. 31
Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen 27

Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort) 28

E

Endpunkt aktivieren 33
Endpunkt deaktivieren 33
Endpunkt entfernen 33
Endpunkt hinzufügen 33
Endpunktdefinition 8
Ereignisprotokollmeldungen 30
Ermittlungsdienst 17
Ermittlungsserver 9
Ermittlungsserver entfernen 33
Ermittlungsserver hinzufügen 33
Exportieren 9-10
Externe DA Server 25

F

Firewall 17, 25

I

Importieren 9-10
Inhalt der Hilfe 4
Instanzzertifikate 12

K

Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll 28
Konto '<Name>' hat keine Berechtigung zum Ausführen der Anwendung. 30

L

Lokaler Ermittlungsdienst (LDS) 17

N

Netzwerkadapter 8

O

OPC Data Access (DA) 4
OPC Foundation 4
OPC UA Configuration Manager 5
OPC UA Lernprogramm 15
OPC Unified Architecture (UA) 4

P

Passwort 6
Port-Nummer 8
Projekteigenschaften - OPC UA 5

R

Registrierungsintervall 10
Remote-Clients 25
Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden 28

S

Serverendpunkte 7
Serverzertifikat erneut ausstellen 33
Sicherheit 6, 15
Sicherheitsrichtlinien 8
Standard-Zertifikat 13

T

Tipps zur Problembehandlung 27

U

Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden 28
Überprüfung 23
Übersicht 4

V

Verbindungsbeispiele 25
Vertrauen 9
Vertrauenswürdige Clients 9
Vertrauenswürdige Server 10
Vertrauenswürdigem Client vertrauen 32
Vertrauenswürdigem Server vertrauen 33
Vertrauenswürdigen Client ablehnen 32
Vertrauenswürdigen Client entfernen 32
Vertrauenswürdigen Client hinzufügen 32
Vertrauenswürdigen Server ablehnen 33
Vertrauenswürdigen Server entfernen 32
Vertrauenswürdigen Server hinzufügen 32
Voraussetzungen 15

Z

Zertifikat 11
Zertifikat anzeigen 9
Zertifikat erneut ausstellen 12
Zertifikat importieren 12-13
Zertifikatanzeige 13
Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird 27